ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Laboratorio di
Sicurezza Informatica

Cifratura di file e filesystem

Andrea Melis
Marco Prandini
Dipartimento di Informatica – Scienza e Ingegneria

Crittare Cartelle e/o File System

- In questa esercitazione useremo due tool principali
  - fscrypt: per crittare cartelle all'interno della stessa partizione in modo da renderli crittati per utenti diversi
  - luks: per creare e crittare un intero file system
- In aggiunta a questi due tool principali verranno usati altri tool secondari, e verrà aggiunto un disco alla macchina dell'esercitazione tramite virtualbox.

Aggiungiamo un utente

- Per prima cosa, aggiungiamo un utente che useremo poi per dimostrare la cifratura delle directory tra diversi utenti
- Prendiamo una shell di root con

```
su -
inserire password gennaio.marzo
```

- Il carattere “-” dopo il su serve a reinizializzare le variabili d’ambiente tra cui PATH.

Aggiungiamo l’utente sec al gruppo sudoers

- A questo punto aggiungiamo un utente

```
useradd -m otheruser
-m specifica che venga creata anche la directory
home
```

- Cambiamo la password

```
passwd otheruser
inserire due volte la nuova password per
l’utente
```

Aggiungiamo l'utente sec al gruppo sudoers

- Abbiamo bisogno che sec possa compiere azioni da utente privilegiato, per cui dobbiamo aggiungerlo ai sudoers
- Per aggiungerlo al gruppo sudo:

```
usermod -aG sudo sec
```

- Per aggiungerlo al file /etc/sudoers.

```
visudo
sec   ALL=(ALL:ALL) ALL
```

Identificare il file system

- Usciamo dalla shell di root con:

```
exit
```

- Identifichiamo il file system sul quale andremo a lavorare.

```
sudo fdisk -l
Disk /dev/sda: 19.8 GiB, 21265121280 bytes, 41533440
sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfcf48969
Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 39438335 39436288 18.8G 83 Linux
/dev/sda2       39440382 41531391  2091010 1021M  5
Extended
```

dev/sda1 è quindi quello che ci interessa!

Identificare il file system

- Usiamo delle variabili per semplificare il lavoro

```
export DEVICE=/dev/sda1
```

- Per configurare un filesystem per supportare la crittografia, prima bisogna controllare che la dimensione del blocco sia uguale alla dimensione della pagina confrontando gli output di getconf PAGE_SIZE e tune2fs -l / dev / device | grep 'Block Size'.
- Se i valori non corrispondono, non si può abilitare la crittografia.

```
getconf PAGE_SIZE
4096
sudo tune2fs -l /dev/$DEVICE | grep 'Block Size'.
Block size:               4096

I valori coincidono, possiamo procedere!
```

Abilitiamo la crittografia

- Possiamo a questo punto abilitare la crittografia sul device con partizione ext4 con:

```
sudo tune2fs -O encrypt $DEVICE
```

- A questo punto è arrivato il momento di installare il tool (più una libreria collegata) che ci servirà per completare l'esercitazione.
- NOTA: Ricordarsi sempre che per poter funzionare il prossimo comando ci deve essere almeno UNA interfaccia di rete della Virtual Machine configurata come NAT.
- Installare i pacchetti con:

```
sudo apt-get install fscrypt libpam-fscrypt

Attendere che i pacchetti vengano installati
```

Configuriamo la pam list

- Creiamo il file /usr/share/pam-configs/keyinit-fix (c'è bisogno di farlo da utente privilegiato). Vi o nano è indifferente

```
sudo nano /usr/share/pam-configs/keyinit-fix
```

- Compiliamo coi seguenti valori per fscrypt

```
Name: keyinit fix
Default: yes -> Policy di default
Priority: 0
Session-Type: Additional
Session:
     optional  pam_keyinit.so force revok
```

- Riconfiguriamo pam affinche usi fcrypt

```
sudo pam-auth-update
scegliere opzione 6
```

Crittiamo una cartella

- Siamo a questo punto pronti per crittare una cartella. Come prima cosa lanciamo il setup iniziale con:

```
sudo fscrypt setup
sudo fscrypt setup
Replace "/etc/fscrypt.conf"? [y/N] y
Customizing passphrase hashing difficulty for this
system...
Created global config file at "/etc/fscrypt.conf".
```

- Successivamente effettuiamo il setup sulla partizione root

```
sudo fscrypt setup /
```

E siamo pronti per crittare una cartella

Crittiamo una cartella

- Creiamo una cartella

```
mkdir encrypted
```

- Crittiamola con fscrypt

```
fscrypt encrypt encrypted

Should we create a new protector? [y/N] N
Selezione il protector generato per sec con la
password di login UNIX "sec"
```

- È possibile durante la configurazione di PAM usare una chiave (cioè una passphrase) nuova invece che la password di sistema.

Cartella Crittata

- A questo punto la cartella è in modalità cifrata. È possibile inserirci dentro tutti i file che vogliamo; a "prima vista" non cambia nulla viene interpretata come una normale cartella.

- Se proviamo però a fare logout e nuovamente login sia con l'utente sec che con l'utente otheruser creato all'inizio vedremo il contenuto della cartella cifrato.

- È possibile quindi fare l'unlock della cartella con

```
fscrypt unlock encrypted

Enter login passphrase for sec:
Inserire password del protector sec, cioè "sec"
```

Cifriamo l'intera home di un utente

- **Possiamo quindi secondo lo stesso principio cifrare l'intera home di un utente. Anche se questa contiene già dei file con i seguenti comandi:**

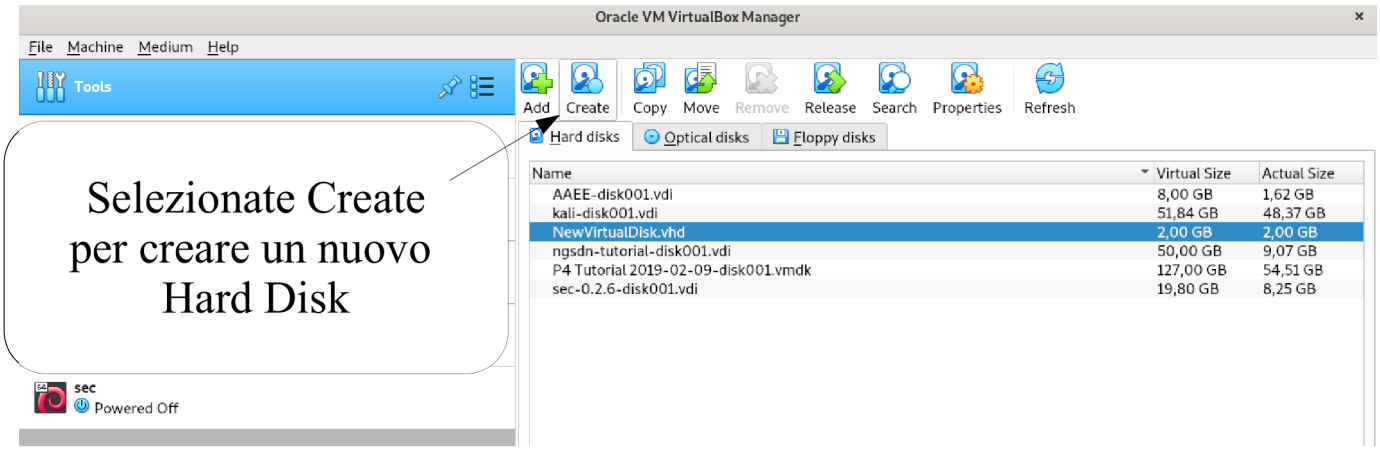
```
su -
export USERNAME=otheruser
mv /home/$USERNAME /home/$USERNAME.bak
mkdir /home/$USERNAME
chown $USERNAME:$USERNAME /home/$USERNAME
fscrypt encrypt /home/$USERNAME --user=$USERNAME // selezionare login di otherusernme e quindi inserire la sua password
rsync -avH --info=progress2 --info=name0 /home/$USERNAME.bak/ /home/$USERNAME/ // è solo per imparare un nuovo tool fa solo la copia con un po di output fatto bene :) installarlo con:
apt install rsync
rm -rf /home/$USERNAME.bak
Ripetere logout/login utenti diversi per verifica
```

E se volessimo cifrare un'intera partizione?

O un'intero disco appena associato alla vostra macchina?

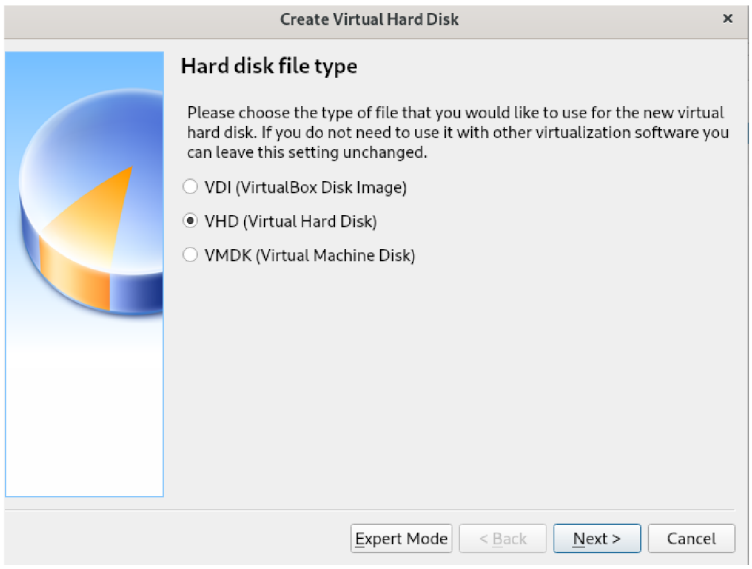
Aggiungiamo un altro disco.

- Il disco attualmente presente nella VM non ha spazio non associato dove poter creare una nuova partizione.
- Creiamo e aggiungiamo quindi un nuovo disco alla VM del laboratorio.
- Spegniamo la macchina
- Cerchiamo nell'interfaccia di Virtualbox la sezione "Media"



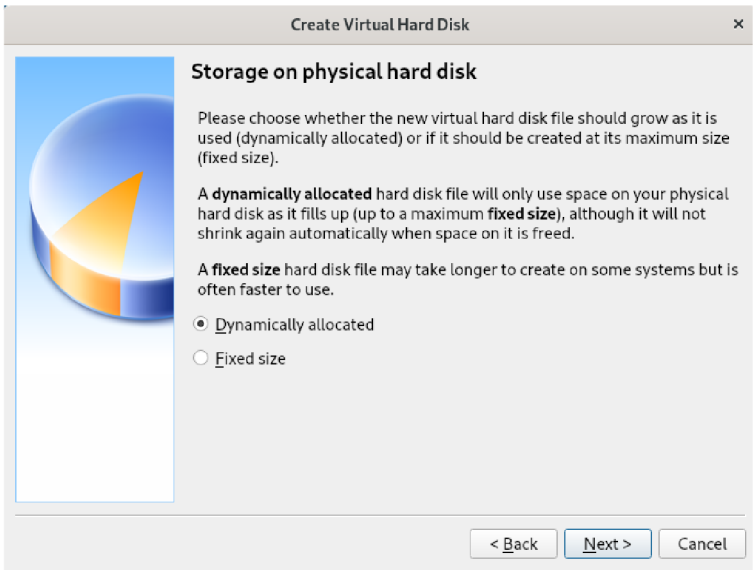
Aggiungiamo un altro disco.

- Selezionate VHD



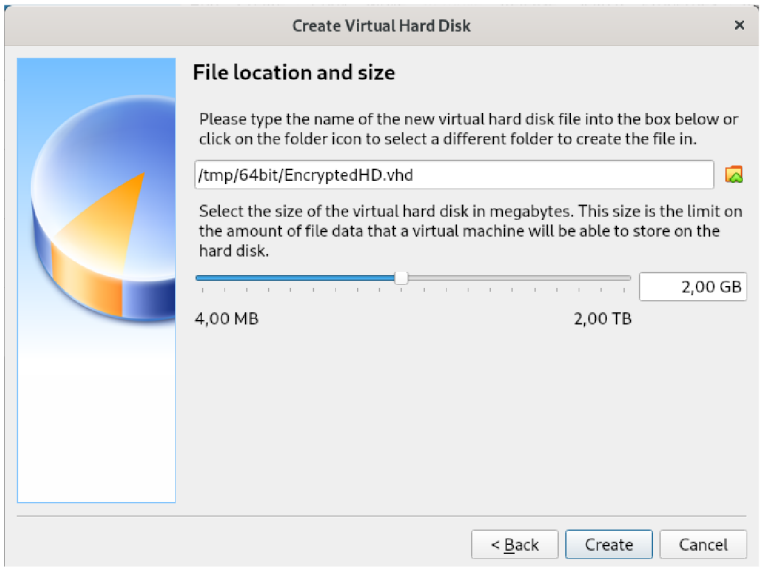
Aggiungiamo un altro disco.

- Selezionate Dynamically allocated



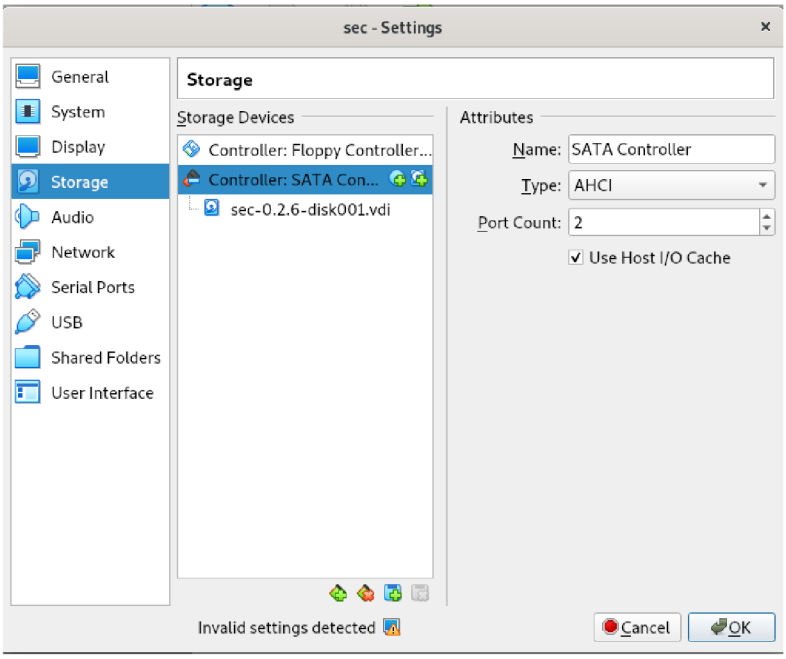
Aggiungiamo un altro disco.

- Selezionate 2 GB come size e dategli nome EncryptedHD.vhd



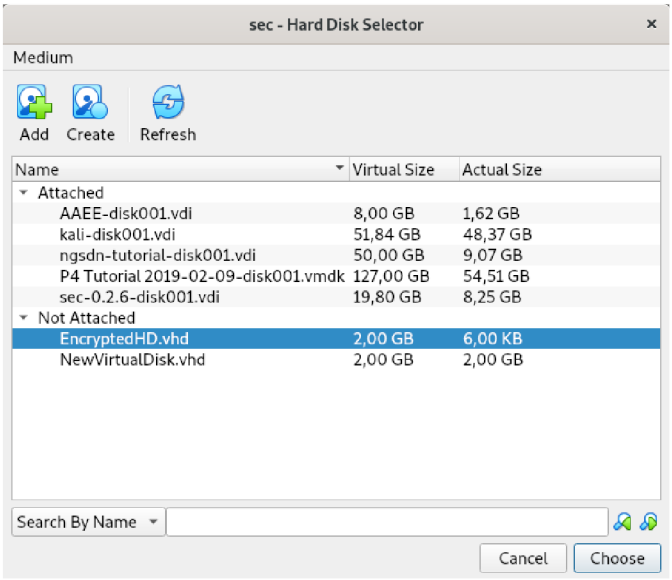
Aggiungiamo un altro disco.

- Dopo di che, andate sulle settings della vostra macchina del laboratorio, poi su Storage, e alla voce Controller: SATA premete sull'icona per aggiungere un HD.



Aggiungiamo un altro disco.

- Selezionate l'HD creato precedente e salvate tutto con OK



Disco Aggiunto.

- Abbiamo quindi aggiunto un nuovo HD alla macchina.
- Riaccendiamo la macchina. Potrebbe metterci qualche secondo in piu del solito al boot.

Crittiamo una partizione

- Come prima cosa, installiamo i pacchetti che ci servono per questa esercitazione.
- Da utente privilegiato.

```
su -
```

- Installiamo il tool che ci serve

```
apt-get install cryptsetup
```

- Accertiamoci che il modulo kernel dm_crypt sia caricato, questo modulo infatti è parte del device mapper serve da supporto a LUKS.

```
modprobe dm_crypt
```

- Installiamoci infine un altro tool (pv) non indispensabile ma che ci verrà comodo più avanti

```
apt-get install pv
```

Creiamo la partizione

- Come prima cosa, vediamo cosa il sistema operativo vede dei dishi. Lanciamo:

```
fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 19.8 GiB, 21265121280 bytes, 41533440
sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfcf48969
```

  - Lo spazio non allocato nel disco aggiunto è in /dev/sdb

Creiamo la partizione

- Creiamo quindi una nuova partizione

```
fdisk /dev/sdb


scelgiamo prima p per vedere le tabelle di partizione
e notare come non sia presente nessuna per sdb


scegliamo quindi n per fare una nuova partizione


scegliamo quindi p per farna una primaria


selezioniamo i valori di default ( premo invio )


scegliamo w per scrivere i cambiamenti richiesti
```

Verifichiamo la partizione creata

- Lanciamo nuovamente fdisk

```
fdisk -l

Device     Boot Start     End Sectors Size Id Type
/dev/sdb1        2048 4194303 4192256   2G 83 Linux
```

LUKS

- Formattiamo ora la partizione per il formato LUKS

```
cryptsetup luksFormat /dev/sdb1
digitare YES
digitare una passphrase
reinserire la passphrase
```

- A questo punto è possibile “aprire” la partizione con luks

```
cryptsetup luksOpen /dev/sdb1  crittata
inserire passphrase
```

- La partizione LUKS è quindi visibile come device mapper

```
ls -l /dev/mapper
```

LUKS

- Ora un piccolo accorgimento. Sovrascriviamo il volume LUKS con zeri per garantire che dall'esterno la partizione venga come insieme di dati casuali. Questo protegge dalla possibilità di ricavare possibili pattern di utilizzo della partizione:

```
pv -tpreb /dev/zero | dd of=/dev/mapper/crittata bs=1M
```

```
dove:
/dev/zero è un file speciale unix che restituisce
tanti NULL byte quanti se ne vuole leggere

bs=1M significa che legge e scrive 1 MB alla volta

per i parametri di pv leggere la man page!
```

LUKS

- A questo punto possiamo creare un file system nella nostra partizione LUKS

```
mkfs.ext4 /dev/mapper/crittata -L crittata
```

- Non ci resta quindi che creare un nuovo punto sul quale montare la partizione e montarla.

```
mkdir /tmp/crit

mount /dev/mapper/crittata /tmp/crit
```

- E' possibile quindi navigare il contenuto della partizione liberamente.

LUKS

- Si può quindi fare l'umount della partizione e chiudere la partizione LUKS

```
umount /tmp/crit

cryptsetup luksClose crittata
```